

The Honorable Brian A. Tsuchida

FILED ENTERED
LOGGED RECEIVED

JAN 04 2016

SEATTLE
CLERK U.S. DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
DEPUTY

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

LONNIE EUGENE LILLARD,
NATHANIEL WELLS,
ERIN TERRIL WILEY, and
MELISA SANDERS,

Defendants.

No. **MJ16-002**

COMPLAINT FOR VIOLATION

Title 18, United States Code, Sections 1344
and 1349

BEFORE Brian A. Tsuchida, United States Magistrate Judge, U.S. District
Courthouse, Seattle, Washington.

The undersigned complainant being duly sworn states:

Count One

(Conspiracy to Commit Bank Fraud)

A. The Offense

1. Beginning in or about July 2014, and continuing until at least September 2015, at Kent, Federal Way, Renton, Seattle, SeaTac, and Tukwila, within the Western District of Washington, and elsewhere, the defendants, LONNIE EUGENE LILLARD, NATHANIEL WELLS, ERIN TERRIL WILEY, and MELISA SANDERS, and others known and unknown, did conspire to knowingly execute a scheme and artifice to defraud

1 KeyBank, Green Dot Bank, Sunrise Bank, and JPMorgan Chase, all of which are
2 financial institutions as defined by Title 18, United States Code, Section 20, and to obtain
3 moneys, funds, and credits owned by and under the custody and control of those financial
4 institutions by means of materially false and fraudulent pretenses, representations, and
5 promises, as further and more particularly set forth below.

6 **B. The Object of the Conspiracy**

7 2. The object of the conspiracy and of the scheme and artifice to defraud was
8 to obtain cash and credit by using point-of-sale (POS) terminals to fraudulently process
9 returns from merchants; to load the funds obtained from the fraudulent returns onto pre-
10 paid debit cards, gift cards, pre-paid credit cards, and other similar cards issued by banks
11 and retailers; and then to withdraw those fraudulently obtained funds by using the pre-
12 paid debit cards, gift cards, pre-paid credit cards, and other similar cards for cash
13 withdrawals at various bank branches and automated teller machines (ATMs) in
14 Washington and elsewhere.

15 **C. Manner and Means of the Conspiracy and Scheme and Artifice to Defraud**

16 3. It was part of the conspiracy and scheme and artifice to defraud for
17 LONNIE EUGENE LILLARD and others known and unknown to obtain POS terminals
18 from merchants in the greater Seattle area and elsewhere.

19 4. It was further part of the conspiracy and scheme and artifice to defraud for
20 LONNIE EUGENE LILLARD and others known and unknown to reprogram the
21 aforementioned POS terminals to change the assigned merchant identification number
22 (merchant ID) to that of a specific retailer or business.

23 5. It was further part of the conspiracy and scheme and artifice to defraud for
24 NATHANIEL WELLS and ERIN TERRIL WILEY, and others known and unknown to
25 obtain pre-paid debit cards, gift cards, pre-paid credit cards, and other similar cards from
26 issuers such as KeyBank, US Bank, Capital One, Sunrise Bank, and others. These pre-
27 paid cards worked similarly to credit cards, but only allowed users to withdraw and/or
28 spend funds that were previously deposited, credited, or "loaded" onto the cards.

1 6. It was further part of the conspiracy and scheme and artifice to defraud that
2 LONNIE EUGENE LILLARD, NATHANIEL WELLS, and others known and unknown
3 would then use the reprogrammed POS terminals from hotel rooms rented for that
4 purpose by MELISA SANDERS and others known and unknown and from other
5 locations to conduct dial-in transactions through the credit card processing network and
6 banking system. During these transactions, LONNIE EUGENE LILLARD,
7 NATHANIEL WELLS, and others known and unknown would process false and
8 fraudulent credits from specified businesses to the cards obtained by NATHANIEL
9 WELLS, ERIN TERRIL WILEY, and others known and unknown. The credits were not
10 authorized by the particular business, and did not reflect returns of merchandise or other
11 legitimate transactions. The transactions caused funds to be transferred from the account
12 of the particular business to the accounts associated with the cards.

13 7. It was further part of the conspiracy and scheme and artifice to defraud that
14 NATHANIEL WELLS, ERIN TERRIL WILEY, MELISA SANDERS, and others
15 known and unknown would take the cards onto which the fraudulent credits were
16 processed, knowing that these funds did not belong to them, and either withdraw those
17 fraudulently obtained funds via ATM in a process referred to as "a cash out" or "cashing
18 out," or use the cards to purchase Western Union money orders, MoneyGrams, other
19 negotiable instruments, or automotive repairs.

20 8. It was further part of the conspiracy and scheme and artifice to defraud for
21 NATHANIEL WELLS, ERIN TERRIL WILEY, and others known and unknown to
22 share the funds they received from these withdrawals or purchases of negotiable
23 instruments with LONNIE EUGENE LILLARD and others known and unknown.

24 All in violation of Title 18, United States Code, Sections 1344 and 1349.

25 ///

26 ///

27

28

1 I, Kevin Brennan, being first duly sworn on oath, do hereby depose and state:

2 **I. INTRODUCTION AND AGENT BACKGROUND**

3 1. I am a Special Agent with the Federal Bureau of Investigation (FBI), and
4 have been since 2006. I am presently assigned to the FBI Seattle Field Office Cyber
5 Task Force. I earned a Bachelor of Science in Computer Science from the University of
6 Notre Dame in 2001 and a Master of Science in Information Technology (Information
7 Security and Assurance track) from Carnegie Mellon University in 2015. I have been
8 assigned by the FBI to work cyber investigations since 2006 in a variety of field offices.
9 I am a Global Information Assurance Certified (GIAC) computer forensics examiner
10 (GCFE) and GIAC incident handler (GCIH). I have received additional specialized
11 training by the FBI in cyber investigations, including the collection and analysis of digital
12 evidence.

13 2. The information set forth in this affidavit consists of information I have
14 gathered and observed firsthand through the course of this investigation to date, as well
15 as information relayed to me by other law enforcement personnel, information from
16 victim statements, interviews of witnesses, and by review and analysis of various
17 financial records. The information in this affidavit is not intended to detail each and
18 every fact and circumstance of the investigation or all information known to me or all the
19 participants involved in the investigation. Rather, this affidavit serves solely to establish
20 that probable cause exists to believe that LONNIE LILLARD, NATHANIEL WELLS,
21 ERIN TERRIL WILEY, and MELISA SANDERS committed Conspiracy to Commit
22 Bank Fraud in violation of Title 18, United States Code, Sections 1344 and 1349.

23 **II. SUMMARY OF THE INVESTIGATION**

24 3. The FBI is investigating LONNIE EUGENE LILLARD, NATHANIEL
25 WELLS, ERIN TERRIL WILEY, MELISA SANDERS, and others known and unknown
26 for a scheme in which they defrauded banks via fraudulent credit card transactions. The
27 total estimated amount of loss associated with the fraudulent transactions is \$1,433,832
28 between July 8, 2014, and October 23, 2015.

1 4. The fraudulent transactions utilized in the conspiracy between LILLARD,
2 WELLS, WILEY, SANDERS, and others known and unknown include fraudulent
3 refunds and fraudulent reversals. I believe both transactions are processed via point-of-
4 sale terminals in the possession of the co-conspirators that are configured to utilize
5 merchant identification numbers that they are not authorized to use.

6 5. A fraudulent refund is a standalone transaction processed by the
7 conspirators in which they instruct the payment processor to take money from the
8 merchant and place the money onto the credit or similar card.

9 6. A fraudulent reversal consists of a series of transactions. The co-
10 conspirators will pose as the merchant (using the merchant ID, which they are not
11 authorized to use) and process a debit or sale using a credit or similar card (typically for
12 \$0.01). The result of this transaction will include an authorization number associated
13 with this completed transaction. The card will then be used at a retailer—either the
14 original merchant or another merchant entirely—for a legitimate purchase for a larger
15 amount (typically hundreds of dollars totaling the remaining balance on the pre-paid
16 card). The co-conspirators will then process an additional transaction fraudulently posing
17 as the same merchant as in the first transaction, instructing the payment processor to
18 “reverse” a transaction. The reversal transaction will provide the authorization number
19 from the first transaction (conducted by the co-conspirators), but will provide the amount
20 of the second (legitimate) transaction. This will effectively cause the amount of the
21 second transaction to be removed from the balance on the card, leaving only the amount
22 charged in the first transaction. The co-conspirators will then repeat these transactions
23 multiple times, artificially inflating the available amount of funds on the card and then
24 spending them. This allows the co-conspirators to spend amounts in excess of the funds
25 legitimately loaded onto the card at the initial time of purchase.

26 7. As detailed below, based on my investigation and the investigation of other
27 law enforcement officers, I submit that probable cause exists to believe that LILLARD,
28 WELLS, WILEY, and SANDERS committed the violation described above. In

1 particular, the FBI investigation has uncovered evidence that LILLARD, WELLS,
2 WILEY, and SANDERS conspired to commit Bank Fraud by agreeing to work together
3 to develop a plan to cause credit card and similar transactions to be drawn against
4 business accounts maintained at a variety of financial institutions to which they had no
5 legitimate access, and then to cause the funds received from these accounts to be
6 withdrawn. These fraudulent transactions caused the theft of money under the control of
7 financial institutions, a bank fraud.

8 III. EXPLANATION OF TERMS AND TECHNOLOGY

9 8. Point-of-sale (POS) terminals are digital devices that scan a magnetic strip
10 on a debit, credit, or gift card and use the information encoded therein to conduct
11 electronic debit, credit, and gift card purchases and refunds. These terminals are
12 commonly found next to a merchant's cash register, and are programmed with the
13 merchant's or other entity's unique information so that a transaction can be processed.
14 During a "purchase," funds are debited from the cardholder's account and credited to the
15 merchant's account. During a "refund," the funds are debited from the merchant's
16 account and credited to the cardholder's account. To conduct a POS transaction, a
17 merchant or customer uses a card equipped with a magnetic strip that is encoded with
18 information and slides that card through a reader mounted or attached to the POS
19 terminal. The POS terminal then uses the card information encoded on the magnetic
20 strip, in conjunction with the merchant's information previously programmed into the
21 POS terminal, to conduct the transaction and transfer the funds. At the time this scheme
22 was executed, the majority of POS terminals in use throughout the United States were
23 programmed to access the banking system via data connections across the Internet, not
24 via dial-in connections over a standard telephone line. In the case of this scheme or
25 artifice to defraud, however, the particular POS terminals used placed dial-in or dial-up
26 calls to the specific processing company.

27 9. A merchant ID is a unique identifier assigned to a business or other entity
28 that need to process debit or credit card transactions. The merchant ID is programmed

1 into a POS terminal to identify the associated retailer or business to which the
2 transactions should be associated. No other password or security mechanism beyond the
3 merchant ID is required to configure a POS terminal to conduct transactions as a specific
4 retailer or business.

5 10. A single business or other entity may have hundreds of merchant IDs, as it
6 will have at least one unique merchant ID for each retail outlet or location where debit
7 and credit card transactions are processed. When a single business has multiple merchant
8 IDs, certain processing companies assign sequential merchant IDs to the business's
9 various outlets. Also, certain businesses print their merchant ID on receipts they generate
10 for their customers at the time of the transaction. Accordingly, sometimes merchant IDs
11 can be directly obtained from a merchant or easily guessed.

12 11. A particular POS terminal is configured to process transactions with only a
13 particular payment processor. To process transactions with multiple payment processors,
14 an individual would need at least one POS terminal for each different payment processor.

15 12. As used here, a payment processor is an intermediary between banks and
16 merchants that processes credit, debit, and certain gift card transactions.

17 **IV. IDENTIFICATION OF INVOLVED ENTITIES**

18 **A. Financial Institutions**

19 13. KeyBank is an FDIC-insured bank headquartered in Cleveland, Ohio, with
20 approximately 1,000 branches nationwide.

21 14. JPMorgan Chase is a multi-national banking and financial services holding
22 company headquartered in New York, New York, with a variety of subsidiaries,
23 including JPMorgan Chase Bank N.A., an FDIC-insured bank, and Chase Paymentech, a
24 payment-processing business.

25 15. Green Dot Corporation is headquartered in Pasadena, California, and is the
26 operator of Green Dot Bank, an FDIC-insured institution that is a leading provider of pre-
27 paid debit cards.

1 16. Sunrise Banks is an FDIC-insured institution headquartered in St. Paul,
2 Minnesota.

3 17. US Bank is a FDIC-insured bank headquartered in Minneapolis, Minnesota,
4 with over 1,000 branches nationwide.

5 **B. Victim Companies**

6 18. The Michaels Companies, Inc., (dba Michaels) is a large retailer of arts and
7 crafts supplies with outlets across the country.

8 19. See's Candies is a Carson, California, headquartered retailer of chocolates
9 and candies, with over 200 retail locations throughout the United States.

10 20. Pep Boys is a Philadelphia, Pennsylvania, headquartered car parts and
11 automotive services retailer with over 800 stores located throughout the United States.

12 21. Sprint is an Overland Park, Kansas, based telecommunications company
13 that provides cellular telephone service, Internet service, and traditional "land line"
14 services. Sprint operates approximately 2,700 retail stores throughout the United States.

15 22. Sam Moon Group (Sam Moon) operates seven total retail stores in Texas,
16 including separate stores focusing on the sale of luggage or home décor.

17 23. Spencer Spirit Holdings, Inc., (Spencer) is a lifestyle retail company that
18 operates two unique national brands—Spencer's (also referred to as Spencer's Gifts) and
19 Spirit Halloween—throughout the United States, Canada, and online. Spencer operates
20 over 650 stores.

21 24. Monroe Dodge Chrysler Jeep Dealership is an automotive dealership
22 located in Monroe, Michigan.

23 25. Chrysler of Forest City is a Forest City, Iowa, based automotive dealership.

24 26. Fuqua Chrysler Dodge Jeep is a Dunkirk, Indiana, based automotive
25 dealership.

26 27. Don Hill Pontiac Jeep is a Kingsport, Tennessee, based automotive
27 dealership.

28. Campbell Ford Lincoln Mercury is a Niles, Michigan, based automotive dealership.

29. Sheridan Nissan LLC is a New Castle, Delaware, based automotive dealership.

30. Bayway Lincoln Mercury is a Houston, Texas, based automotive dealership.

31. Cash America International, Inc. is a Fort Worth, Texas, headquartered company that operates approximately 850 pawn shops and approximately 80 check-cashing stores located throughout the United States, including the Superpawn, Cash America Pawn, and Cashland.

32. Kelly-Moore Paint Company is a paint company headquartered in San Carlos, California, that operates retail paint stores located throughout the United States.

33. Hometown Buffet is one of several restaurant brands operated by Ovation Brands and headquartered in Greer, South Carolina. Hometown Buffet has approximately 168 restaurants located in the United States.

34. Quiznos is a sub sandwich restaurant offering sandwiches, subs, salads, soups, box lunches, and catering services.

35. Little Caesars Pizza is a Detroit, Michigan, based carry-out pizza chain. Little Caesars operates carry-out pizza chains globally and is the third largest pizza chain in the United States.

C. Payment Processors

36. Chase Paymentech is a payment processor that receives transactions processed by a variety of merchants either directly or via other payment processing companies. Chase Paymentech is a subsidiary of JPMorgan Chase.

37. Vantiv is a Cincinnati, Ohio, based payment processor that processes transactions on behalf of merchants and automated teller machines.

38. INCOMM is an Atlanta, Georgia, based payment processor that processes transactions on behalf of merchants.

1 **V. DETAILS OF THE INVESTIGATION**

2 39. In or about October 2014, FBI Seattle received information from a fraud
3 investigator employed by KeyBank regarding a scheme in which individuals possessing
4 pre-paid KeyBank debit cards were having fraudulent credits loaded onto the cards from
5 businesses located throughout the United States, then withdrawing the funds at KeyBank
6 ATMs using KeyBank cards. The aforementioned KeyBank prepaid debit cards were
7 "KeyBank Possibilities" cards and were not linked to any other KeyBank checking or
8 savings account. All of the identified fraudulent transactions provided by the KeyBank
9 fraud investigator had been processed by Chase Paymentech between July and September
10 2014. KeyBank Investigators identified these transactions due to the debit cards not
11 having corresponding debits to the credits that were received. Approximately \$300,000
12 in fraudulent credits were processed onto pre-paid debit cards issued by KeyBank.
13 KeyBank also provided FBI-Seattle with the names and some identifiers of individuals
14 who had pre-paid debit cards issued in their names onto which the fraudulent transactions
15 had been processed. Many of the individuals had numerous cards associated with them.
16 WILEY was the named individual associated with three of the cards onto which
17 fraudulent credits were processed and funds withdrawn; WELLS was the named
18 individual associated with eleven of the cards.

19 40. KeyBank provided FBI-Seattle with a photograph of one of the individuals
20 who had made a series of withdrawals at a drive-up ATM using a number of the pre-paid
21 debit cards onto which the fraudulent returns had been loaded, along with a photograph
22 of the license plate of the car being driven by that individual during the transactions. The
23 individual in the photograph has not yet been identified.

24 41. FBI Seattle determined, through a check of records held by the Washington
25 State Department of Licensing, that the pictured vehicle is registered to "Michael."
26 According to LILLARD's Federal Bureau of Prisons authorized contacts list, LILLARD
27 lists both "Michael" and WILEY as LILLARD's siblings.
28

1 42. In October 2014, I learned that the United States Secret Service had
2 previously investigated a similar scheme approximately eight years prior, in which
3 "Michael," LILLARD, WELLS, and WILEY had all been suspects, and that LILLARD
4 may have been recently released from federal prison after serving time for his
5 involvement in another similar scheme prosecuted out of the District of Nevada. I later
6 confirmed that LILLARD had in fact been released on June 2, 2014.

7 43. In October or November 2014, Chase Paymentech advised FBI-Seattle that
8 the fraud scheme was continuing, and provided information that the fraudulent credits
9 were being processed through POS terminals via numerous consecutive dial-up
10 transactions. Chase Paymentech also provided information identifying the various
11 merchants who had been victimized by the fraudulent returns. One of these merchants
12 was Michaels.

13 44. In November 2014, FBI Special Agent (SA) Joshua Michaels, FBI Forensic
14 Accountant (FoA) Bryan Snead, FBI Intelligence Analyst (IA) Reginald Chapman, and I
15 interviewed employees of Michaels (the company) regarding fraudulent credits processed
16 between approximately October 28, 2014, and November 15, 2014, using Michaels'
17 merchant IDs. These fraudulent credits were processed through Chase Paymentech to US
18 Bank prepaid cards, among others. Later investigation revealed a total of approximately
19 176 transactions totaling approximately \$84,208. The majority of these transactions
20 occurred after business hours.

21 45. In December 2014, SA Michaels, FoA Snead, IA Chapman and I
22 interviewed and obtained information from fraud investigators of JPMorgan Chase. They
23 advised that, based on their analysis of transaction patterns (including consecutive dial-in
24 refund transactions processed after normal business hours) and communications with
25 their merchant-clients, Chase Paymentech had processed fraudulent credits pursuant to
26 this scheme using merchant IDs belonging to Michaels (the company), Sprint, Quiznos,
27 Pep Boys, and others. At that time, JPMC estimated the fraudulent transaction totals
28 processed by Chase Paymentech as approximately \$685,000. That number later grew to

1 \$897,000 as the scheme continued and as more merchant-victims were identified.

2 JPMorgan Chase was able to provide FBI-Seattle with some of the phone numbers (caller
3 IDs) that were used to dial in to its payment system to process the fraudulent credits.

4 46. Using publicly available sources, FBI-Seattle identified the phone numbers
5 provided by JPMorgan Chase as belonging to hotels in the greater Seattle area. FBI-
6 Seattle contacted those area hotels and obtained guest registry information from each for
7 the period of time during which the hotel's phones were used to process the fraudulent
8 credits. In each case, the registry showed that an individual associated with LILLARD
9 was a guest at the hotel during that time period. In one case, the hotel was able to
10 identify the particular room's phone that was used to make the dial-in transactions. That
11 room was rented at that time by SANDERS.

12 47. During a period of time between approximately February 2015 and
13 approximately June 2015, when LILLARD was temporarily residing in the greater Seattle
14 area and purportedly looking for employment, LILLARD informed his federal probation
15 officer that he would be staying with SANDERS. LILLARD also listed SANDERS as a
16 sibling on his authorized contact list with the Federal Bureau of Prisons during his period
17 of incarceration.

18 48. According to information provided by Western Union, an individual using
19 the name Edward Dubai sent approximately \$13,023 via 18 separate wire transfers to
20 SANDERS between August 1, 2014 and October 7, 2014. According to BOP records,
21 Edward Dubai is a known alias of LILLARD. The amount transferred exceeds
22 LILLARD's legitimate income during this time period that is known to the investigative
23 team. I believe that these wire transfers include the disbursement of the fruits of the
24 conspiracy described herein.

25 49. According to the information provided by JPMorgan Chase, on or about
26 July 23, 2014, 18 total fraudulent credits totaling \$17,460 were processed during a period
27 of approximately seven hours beginning at approximately 2:52 a.m. These credits were
28 issued to the cards via transactions originating from the telephone number 206-878-0387.

1 This phone number belongs to Westview Motel in Des Moines, Washington. A review of
2 the guest registry for July 23, 2014, shows that SANDERS was a registered guest at that
3 time. Of these 18 fraudulent transactions, eight transactions, totaling \$5,200, were
4 processed using merchant IDs belonging to Sam Moon Group, located in Texas. The
5 other ten transactions, totaling \$12,260, were processed using merchant IDs belonging to
6 See's Candies locations in California, Oregon, and Washington.

7 50. According to information provided by Wells Fargo, on or about July 23,
8 2014, a debit card ending in 2175 was issued by Wells Fargo to an individual that
9 presented identification at account opening belonging to SANDERS. On or about August
10 19, 2014, this debit card received three point-of-sale "purchase return" transactions
11 totaling \$1,750. The merchant ID used during these transactions was assigned to a
12 Quizno's in Oakland, CA. There are no listed corresponding purchases made with the
13 card at any Quizno's. I believe that the transactions listed were fraudulent and part of the
14 scheme described herein.

15 51. According to the information provided by JPMorgan Chase, on or about
16 December 9, 2014, 148 total fraudulent credits, totaling \$67,348, were processed during a
17 period of approximately four hours beginning at 1:35 a.m. These 148 total transactions,
18 totaling \$67,348, all were processed using merchant IDs belonging to Pep Boys stores
19 located throughout the state of California. These credits were issued to the cards via
20 transactions originating from the telephone number 206-248-8304. This phone number
21 belongs to Coast Gateway Hotel in SeaTac, Washington. A review of the guest registry
22 for December 9, 2014, shows that SANDERS was a registered guest at that time. In
23 addition, a review of telephone records for calls originating from the room rented by
24 SANDERS showed two telephone calls totaling approximately 17 minutes in length to
25 206-465-1540, a cellular telephone number subscribed to by WELLS. These calls to
26 WELLS were made approximately 29 minutes prior to approximately 200 telephone calls
27 made from the room rented by SANDERS to 1-800-886-1764, a telephone number used
28 by Chase Paymentech to process dial-up credit and debit card transactions. These

1 telephone calls were extremely short, usually lasting less than 20 seconds, and are
2 consistent with dial-up transactions originating from a POS terminal, which can be
3 processed in less than 20 seconds. The discrepancy between approximately 200 phone
4 calls and 148 known fraudulent transactions can be explained by either a number of
5 transactions not being flagged as fraudulent, errors made by the user in inputting card
6 numbers, so that the transaction would be declined, or the POS terminal being
7 disconnected for any number of reasons prior to completion of the transaction.
8 According to Coast Gateway Hotel employees, they have a policy of requiring guests to
9 provide identification at check-in.

10 52. According to the information provided by JPMorgan Chase, on or about
11 December 20, 2014, 141 total fraudulent credits, totaling \$66,081, were processed during
12 a period of approximately five hours beginning at 12:55 a.m. These credits were issued
13 to the cards via transactions originating from the telephone number 425-226-7600. This
14 phone number belongs to Quality Inn in Renton, Washington. A review of the guest
15 registry for December 20, 2014, shows that both SANDERS and WELLS were registered
16 guests at that time. All 141 transactions, totaling \$66,081, were processed using
17 merchant IDs belonging to Sprint retail stores located throughout the United States.

18 53. According to the information provided by JPMorgan Chase, on or about
19 January 14, 2015, 70 total fraudulent credits, totaling \$90,969, were processed. These
20 credits were issued to the cards via transactions originating from the telephone numbers
21 509-962-6888, 509-962-6881, 509-962-6889, and 509-962-6880. All of these phone
22 numbers belong to Super 8 Motel in Ellensburg, Washington. A review of the guest
23 registry for January 14, 2015, shows that both SANDERS and WELLS were registered
24 guests at that time. Forty transactions, totaling \$53,485, were processed using a merchant
25 ID belonging to Monroe Dodge Chrysler Jeep located in Monroe, Michigan. Thirty
26 transactions, totaling \$37,484, were processed using a merchant ID belonging to Chrysler
27 Forest City located in Forest City, Iowa.
28

1 54. According to the information provided by JPMorgan Chase, on or about
2 January 15, 2015, 95 total fraudulent credits, totaling \$101,840, were processed. These
3 credits were issued to the cards via transactions originating from the telephone numbers
4 509-962-6888, 509-962-6881, 509-962-6889, and 509-962-6880, the same phone
5 numbers listed above regarding the January 14, 2015, transactions. These phone
6 numbers belong to Super 8 Motel in Ellensburg, Washington. A review of the guest
7 registry for January 15, 2015, shows that SANDERS was a registered guest at that time.
8 Of these 95 transactions, two transactions, totaling \$40, were processed using a merchant
9 ID belonging to Chrysler Forest City located in Forest City, Iowa. Sixty-one
10 transactions, totaling \$66,700, were processed using a merchant ID belonging to Don Hill
11 Pontiac Jeep located in Kingsport, Tennessee. Thirty-two transactions, totaling \$35,100,
12 were processed using a merchant ID belonging to Fuqua Chrysler Dodge Jeep RAM in
13 Dunkirk, Indiana.

14 55. LILLARD listed WELLS on his authorized contact list with the Federal
15 Bureau of Prisons, including his email address and his phone number. I confirmed from
16 records of the telephone service provider that WELLS is the subscriber for that phone
17 number. A review of LILLARD's telephone calls while he was incarcerated show 11
18 telephone calls from LILLARD to WELLS.

19 56. From July 1, 2014, to December 23, 2014, WELLS made approximately
20 3,000 phone calls and text messages to a particular cell phone number known to
21 investigators, representing the fourth most common number that WELLS contacted
22 during this period. Two different witnesses have identified this cell phone number to
23 investigators as belonging to LILLARD. LILLARD was released from incarceration on
24 June 2, 2014.

25 57. On or about December 26, 2014, WELLS received fraudulent credits to two
26 Capital One credit cards (not pre-paid cards) issued in his name and ending in 3090 and
27 2892. Two credits of \$400 each were processed using merchant IDs belonging to
28 Spencer Gifts stores located in Illinois and Kansas to his card ending in 3090. Two

1 credits of \$500 each were processed using the same Spencers Gifts merchant IDs to his
2 card ending in 2892. These transactions were processed via Chase Paymentech, which
3 later identified these transactions as fraudulent. These credits were issued to the cards via
4 transactions originating from the telephone number 425-226-4100. This phone number
5 belongs to SpringHill Suites, Renton, Washington. A review of the guest registry for
6 December 25, 2014, shows that WELLS was a registered guest from the night of
7 December 25, 2014, to December 26, 2014. The guest registry also showed that the
8 aforementioned Capital One credit card belonging to WELLS ending in 2892 was used to
9 pay for the room and associated incidental charges at the SpringHill Suites.

10 58. LILLARD listed WILEY as a sibling on his authorized contact list with the
11 Federal Bureau of Prisons during the period of his incarceration. WILEY was also in
12 contact with WELLS, exchanging approximately 150 telephone calls with WELLS
13 between July 1, 2014, and December 23, 2014.

14 59. On or about July 8, 2014, 17 total fraudulent credits totaling approximately
15 \$7,148 were processed during an approximately four hour period beginning at 4:41 a.m.
16 These credits were issued to the cards via transactions originating from the telephone
17 number 206-248-1000. This phone number belongs to the Crowne Plaza in Seattle,
18 Washington. A review of the guest registry for July 7, 2014, shows that WILEY was a
19 registered guest at that time. Of these 17 transactions, two transactions, totaling
20 approximately \$671, were processed using a merchant ID belonging to Superpawn #1669
21 located in Peoria, Arizona. Nine transactions, totaling approximately \$3,916, were
22 processed using merchant IDs belonging to various Cashland Financial Services stores
23 located throughout the United States. Four transactions, totaling approximately \$1,686,
24 were processed using merchant IDs belonging to Cash America Pawn stores located
25 throughout the United States.

26 60. In or about August through September 2014, 20 Key Possibility Cards were
27 issued in the name of "Shumika" to an applicant using "Shumika"'s social security
28 number. Several of these cards received credits from auto dealerships throughout the

1 United States, as described below and as provided to investigators by KeyBank. On
2 September 11, 2014, "Shumika" received fraudulent credits to a card ending in 82323.
3 One credit was received at 3:21 a.m. from Sheridan Nissan LLC located in New Castle,
4 Delaware, totaling \$2,000.

5 61. On the same day, the same card ending 82323 belonging to "Shumika" had
6 three debit transactions totaling \$1,480. At 5:10 a.m., \$500 was withdrawn from the
7 Rainier Beach KeyBank ATM. At 5:11 a.m., \$500 was withdrawn from the Rainier
8 Beach KeyBank ATM. At 5:12 a.m., \$480 was withdrawn from the Rainier Beach
9 KeyBank ATM.

10 62. On September 11 and September 12, 2014, "Shumika" received fraudulent
11 credits to a card ending in 82364 according to KeyBank. On September 11, 2014, one
12 credit was received at 4:05 a.m. from Bayway Lincoln Mercury located in Houston,
13 Texas, totaling \$2,000.

14 63. On September 11 and September 12, 2014, a card ending 82364 belonging
15 to "Shumika" had four debit transactions totaling \$1,480. Sequentially, these transactions
16 were as follows: On September 11, 2014, at 5:09 a.m., \$480 was withdrawn from the
17 Renton branch KeyBank ATM. At 10:46 p.m., \$300 was withdrawn from an ATM
18 within Walmart store #58 located in Portland, Oregon. On September 12, 2014, at 2:03
19 a.m., \$500 was withdrawn from the Hayden Island KeyBank ATM located in Portland,
20 Oregon. At 6:18 a.m., \$200 was withdrawn from the Vancouver Main KeyBank ATM
21 located in Vancouver, Washington.

22 64. In July 2015, FBI Task Force Officer (TFO) and Kirkland Police
23 Department Detective Derek Hill and IA Chapman interviewed two individuals
24 associated with this scheme, "J" and "E." J and E acknowledged their participation in the
25 aforementioned scheme. J has four felony convictions, three of which relate to
26 Possession or Trafficking of Stolen Property and the fourth is for Possession of a
27 Controlled Substance. E has no known felony convictions.
28

1 65. J's participation in the scheme described herein included acting as a driver
2 for LILLARD. J also registered hotel rooms under his name from which fraudulent
3 transactions occurred. J was also aware of hotel rooms rented by WELLS and
4 SANDERS from which fraudulent transactions occurred. J recruited additional
5 participants for LILLARD and introduced E to LILLARD. E was not knowingly an
6 active participant, but witnessed LILLARD and WELLS utilizing a POS terminal to load
7 debit cards.

8 66. J explained that LILLARD was the leader of the scheme, and confirmed
9 that LILLARD was the one who programmed and used the POS terminals to fraudulently
10 load credits onto the cards. J and E both described LILLARD using POS terminals to
11 process fraudulent credit and other card transactions while WELLS was present. J
12 described LILLARD as carrying the cards onto which credits would be fraudulently
13 loaded in a binder similar to the type used to carry baseball cards. J said this binder
14 would be in LILLARD's possession at all times.

15 67. Throughout the scheme described herein, J was present in hotel rooms
16 located throughout the Western District of Washington when LILLARD "swiped" credit
17 cards through POS terminals for the purposes of conducting fraudulent refund
18 transactions.

19 68. Throughout the scheme described herein, J would drive LILLARD, who J
20 described as the leader of the scheme, to hotels in the Western District of Washington and
21 elsewhere. J said the rooms were never rented by LILLARD or in LILLARD's own
22 name. LILLARD would then utilize the hotel room that had been rented by others known
23 and unknown. LILLARD would carry POS terminals with him into the room and
24 conduct fraudulent refund transactions.

25 69. J stated that in addition to rooms rented by J for LILLARD, SANDERS
26 would also rent rooms for LILLARD for the purposes of conducting the fraud described
27 herein. J stated that SANDERS was "always good for helping a brother out."
28

1 70. On or about January 23, 2015, LILLARD, WELLS, and another known
2 individual entered a hotel located in Tukwila, Washington, for the purposes of conducting
3 fraudulent POS transactions. E saw LILLARD in possession of POS terminals that E
4 knew to be used by LILLARD for such transactions, and saw LILLARD "swiping" cards
5 through the POS terminal.

6 71. During the course of the scheme described herein, LILLARD sent a text
7 message via cellular telephone to J. This text message contained an image of a bed
8 covered with a large number of money orders. TFO Hill and IA Chapman have
9 reviewed this text message and photograph. On or about February 9, 2015, LILLARD
10 utilized 17 money orders in various amounts under \$1,000 to pay a total of \$7,572.98 on
11 rent for an office space located in Ellensburg, Washington.

12 72. In July and August 2015, employees of Green Dot Corporation and
13 KeyBank provided information regarding fraudulent refund transactions in the above
14 scheme. The KeyBank investigator provided surveillance photographs of an individual
15 withdrawing the funds fraudulently loaded onto KeyBank cards via ATM, including an
16 individual who appears to be WILEY. A Fred Meyer investigator provided surveillance
17 video showing the same individual appearing to be Wiley conducting a transaction on the
18 same date as the KeyBank ATM withdrawal wearing the same clothing. These
19 transactions involving a card ending in 02451 are discussed in more detail in paragraphs
20 90, 92, 96, and 98.

21 73. In July 2015, an employee of Fred Meyer provided surveillance footage of
22 an individual who appears to be WILEY making purchases of Western Union money
23 orders and wearing the same clothing as in the surveillance footage provided by
24 KeyBank. This transaction and video is discussed in more detail in paragraph 95.

25 74. On or about June 2, 2014, LILLARD was released from the custody of the
26 United States Bureau of Prisons after serving a sentence for wire fraud, conspiracy to
27 commit wire fraud, and other charges for his involvement in a scheme similar to that
28 described herein, previously charged in the District of Nevada (under 2:06CR00291PMP-

1 001) that resulted in a sentence of 105 months. The scheme described herein began in
2 July 2014.

3 75. I obtained recordings of telephone conversations made by United States
4 Bureau of Prisons inmate "Marcus," who has been incarcerated on felony charges related
5 to his participation in the prior scheme for which LILLARD served a sentence in federal
6 prison as described earlier, with a release date of October 5, 2015. In one phone call on
7 March 5, 2015, "Marcus" spoke to LILLARD, who described to "Marcus" how "these
8 niggers went through forty thousand and then they count on my motherfucking money"
9 and that "Erin went through twelve thousand in one week," which I believe refers to
10 WILEY. LILLARD further stated that these individuals "ain't committed to the cause
11 like me." LILLARD said that he had been busy "ripping and running," which I believe
12 means conducting activities in furtherance of the scheme described herein. LILLARD
13 said that unspecified individuals were returning to the same spot "fifteen motherfucking
14 times" to purchase Western Union money orders and were told by the employee that they
15 would have to pay cash for the Western Union money orders in the future. LILLARD
16 described how he told the unspecified individuals that Western Union locations have
17 reporting thresholds for individuals conducting transactions in excess of a certain amount.
18 During this call, "Marcus" offered to "do everything" and allow LILLARD to "sit back
19 and relax" once "Marcus" was released from prison.

20 76. Investigators obtained surveillance video showing LILLARD entering a
21 Walgreens store located in Renton, Washington, on June 23, 2015. LILLARD entered
22 the store with an individual known to investigators, M. In the aforementioned interview
23 with J, J told investigators that he introduced M to LILLARD and that M had traveled to
24 Seattle on June 23, 2015, to work with LILLARD. While in the store, LILLARD and M
25 are seen at a Western Union kiosk conducting a transaction. LILLARD exited the store,
26 at which time M completed the transaction with a Walgreens associate. A card ending
27 5052 was used to purchase a \$300 Western Union wire transfer in the name of James
28 Jerry Jones payable to LILLARD. Associated with this purchase was a \$24 service fee

1 for a grand total of \$324.00. According to Western Union records, this wire was received
2 on June 27, 2015, at Check into Cash #11022 located in Vancouver, Washington.

3 77. Investigators obtained surveillance video showing LILLARD entering
4 Check into Cash #11022 on June 27, 2015, and receiving the \$300.00 in funds from the
5 June 23, 2015, Western Union wire transfer. The card ending in 5052 is a Walmart
6 Variable Happy Birthday VISA gift card that was purchased in Renton, Washington, and
7 activated on June 22, 2015, at approximately 7:45 a.m. with a balance of \$500.00. These
8 gift cards are issued through Sunrise Bank and are managed by Green Dot Bank.
9 Between June 23, 2015, and June 25, 2015, the card ending in 5052 received 37
10 fraudulent debits totaling approximately \$14,996. Green Dot Bank verified the actual
11 loss associated to the card 5052 to be approximately \$13,033. Green Dot Bank verified
12 that it is the victim bank for all fraudulent activity associated with this card. Green Dot
13 Bank also verified that the card ending in 5052 received funds by fraudulently
14 authorizing reversals using the merchant ID belonging to Hometown Buffet store #0302
15 located in Happy Valley, Oregon.

16 78. Investigators obtained surveillance video from June 26, 2015, showing
17 LILLARD conducting a transaction at Fred Meyer store #360 located in Portland,
18 Oregon. According to Western Union records, a Western Union wire transfer was
19 purchased in the amount of \$976 by LILLARD and payable to Ester Jordan. According
20 to records received from Fred Meyer, this purchase was made by splitting the cost across
21 two separate cards. A card ending in 2760 was charged \$476.13 and a card ending in
22 2588 was charged \$499.87.

23 79. The card ending in 2760 is a Walmart Variable Presents VISA gift card that
24 was purchased in Vancouver, Washington, and activated on June 26, 2015, at
25 approximately 8:07 a.m. with a balance of \$500.00. These gift cards are issued through
26 Sunrise Bank and are managed by Green Dot Bank. Between the dates of June 26, 2015,
27 and June 29, 2015, the card ending in 2760 received 56 fraudulent debits totaling
28 approximately \$25,829. Green Dot Bank verified the actual loss associated to the card

1 ending in 2760 to be approximately \$23,399. Additionally, Green Dot Bank verified that,
2 because the above-mentioned transactions occurred over a weekend, the cardholder was
3 able to take advantage of their processing system by continuously charging fraudulent
4 debits to this card even after the initial \$500.00 purchase amount was spent. Green Dot
5 Bank verified that it is the victim bank for all fraudulent activity associated with this card.
6 Green Dot Bank also verified that the card ending in 2760 received funds by fraudulently
7 authorizing reversals using the merchant ID numbers belonging to Hometown Buffet
8 store #0313 located in Vacaville, California, and Old Country Buffet store #0314 located
9 in Mesa, Arizona.

10 80. The card ending in 2588 is a Walmart Variable Presents VISA gift card that
11 was purchased in Vancouver, Washington, and activated on June 26, 2015, at
12 approximately 8:03 a.m. with a balance of \$500.00. These gift cards are issued through
13 Sunrise Bank and are managed by Green Dot Bank. Between the dates of June 26, 2015,
14 and June 29, 2015, the card ending in 2588 received approximately 54 fraudulent debits
15 totaling approximately \$24,545. Green Dot Bank verified the actual loss associated to
16 card 2588 to be approximately \$20,078. Additionally, Green Dot Bank again verified
17 that, because the above-mentioned transactions occurred over a weekend, the cardholder
18 was able to take advantage of their processing system by continuously charging
19 fraudulent debits to this card even after the initial \$500.00 purchase amount was spent.
20 Green Dot Bank verified that it is the victim bank for all fraudulent activity associated
21 with this card. Green Dot Bank also verified that card ending in 2588 received funds by
22 fraudulently authorizing reversals from June 26, 2015, to June 29, 2015, using the
23 merchant ID numbers belonging to Hometown Buffet store #0313 located in Vacaville,
24 California, and Old Country Buffet store #0314 located in Mesa, Arizona.

25 81. Investigators obtained surveillance video from June 26, 2015, showing
26 LILLARD conducting a transaction at Fred Meyer store #255 located in Portland,
27 Oregon. According to Western Union records, a Western Union wire transfer was
28 purchased by LILLARD for \$987.98 payable to Ester Jordan. According to records

1 received from Fred Meyer, the card ending in 2760 was charged \$497.98 and the card
2 ending in 2588 was charged \$490. Both cards were loaded and debited as described
3 above.

4 82. Investigators obtained surveillance video from June 26, 2015, showing
5 LILLARD conducting a transaction at Fred Meyer store #150 located in Portland,
6 Oregon. According to Western Union records, a Western Union wire transfer was
7 purchased by LILLARD for \$976 payable to Juanita Booker. According to records
8 received from Fred Meyer, the card ending in 2760 was charged \$486 and the card
9 ending in 2588 was charged \$490. Both cards were loaded and debited as described
10 above.

11 83. Investigators obtained surveillance video from September 8, 2015, showing
12 LILLARD conducting transactions at Fred Meyer store #023 located in Bellevue,
13 Washington. According to INCOMM and Fred Meyer records, a card ending in 0081
14 was charged \$494.95 and a card ending in 3096 was charged \$494.95. Fred Meyer
15 transaction receipt records show these purchases were for two MasterCard Variable gift
16 cards. Each card was initially loaded with \$489.00, and each card required the payment
17 of a \$5.95 activation fee. This transaction occurred at approximately 3:23 p.m. At
18 approximately 5:19 p.m. on September 8, 2015, the cards ending in 3096 and 0081 were
19 both used at the Walmart store #3098 located in Bellevue, Washington. Investigators
20 obtained surveillance video from Walmart showing LILLARD conducting a transaction
21 using each card to make a \$490.00 purchase. According to Walmart transaction/receipt
22 records, cards ending in 3096 and 0081 were used to purchase iTunes gift cards.

23 84. At approximately 6:13 p.m. on the same day, the card ending 3096 was
24 used at the QFC #5822 (Quality Food Center) located in Bellevue, Washington.
25 Investigators obtained surveillance video from QFC showing LILLARD conducting a
26 transaction using the card ending in 3096 to make a \$989.90 purchase. According to
27 QFC transaction/receipt records, the card ending in 3096 was used to purchase two
28

1 \$489.00 MasterCard gift cards. There was an additional \$11.90 in activation fees
2 charged in total.

3 85. INCOMM has verified that the cards ending in 3096 and 0081 are Walmart
4 One Vanilla MasterCard Variable cards that were issued through Bancorp, Inc., and are
5 managed by INCOMM. The card ending in 3096 was purchased on September 7, 2015,
6 at approximately 6:01 p.m. with an initial load of \$495.00. The card ending in 0081 was
7 purchased on September 7, 2015, at approximately 6:11 p.m. with an initial load of
8 \$495.00. On September 8, 2015, the card ending in 3096 received 15 fraudulent reversals
9 totaling \$6,801.50 with an actual loss of \$5,811.50. On September 8, 2015, the card
10 ending in 0081 received 14 fraudulent reversals totaling \$6,339.95 with an actual loss of
11 \$4,359.95. INCOMM verified that the card ending in 0081 received funds by
12 fraudulently authorizing reversals using the merchant ID belonging to Little Caesars store
13 #0013 located in North Richland Hills, Texas. INCOMM verified that the card ending in
14 3096 received funds by fraudulently authorizing reversals using the merchant ID
15 belonging to Home Town Buffet store #0252 located in Westchester, California.

16 86. These transactions are summarized in the following table:

17 Date	Time	Activity
18 Sept. 7, 2015	9:01-9:11 p.m.	Cards ending in 0811 and 3096 are activated and
19		loaded with \$495 each
20 Sept. 8, 2015	10:26 a.m.-	Cards ending 0811 and 3096 are used by unknown
21	2:46 p.m.	individuals for purchases and then loaded through
22		fraudulent reversals
23 Sept. 8, 2015	3:23 p.m.	LILLARD on video using both cards at Fred Meyer
24 Sept. 8, 2015	3:27-3:32 p.m.	Cards ending 0811 and 3096 loaded by fraudulent
25		reversals
26 Sept. 8, 2015	5:19 p.m.	LILLARD on video using both cards at Walmart
27 Sept. 8, 2015	5:24-5:26 p.m.	Cards ending 0811 and 3096 loaded by fraudulent
28		reversals

1 Sept. 8, 2015	2 6:13 p.m.	3 LILLARD on video using card 3096 at QFC
-----------------	-------------	---

4 87. During these aforementioned transactions—the Western Union purchase at
5 Walgreens on June 23, 2015, the Western Union purchases at three different Fred Meyer
6 stores on June 26, 2015, and the September 8, 2015, purchases at Fred Meyer and
7 Walmart—LILLARD is depicted on surveillance video holding a binder similar to the
8 binder described by J.

9 88. On April 9, 2015, LILLARD made a purchase at a Ben Bridge Jeweler
10 store located in Seattle, Washington. The \$900 purchase of a gift card was split across
11 two prepaid credit cards. Ben Bridge employees later determined that the cards that
12 made this purchase were not valid. A Ben Bridge employee provided two surveillance
13 stills of an individual I believe to be LILLARD with a binder similar to the binder
14 described by J.

15 89. On July 31, 2015, KeyBank issued a card ending in 78558 to “Q.T.” On
16 August 2, 2015, a total of 18 fraudulent credits from Papa Murphy’s ranging between
17 \$199.83 and \$199.99 were made to the card totaling approximately \$3,598. On August 2,
18 2015, the card mentioned above issued to “Q.T.” was used to place two separate online
19 orders for a total of three pairs of Nike shoes. The shipping information listed for both
20 orders included WELLS’s name and the order information included the telephone
21 number belonging to WELLS.

22 90. Investigators obtained surveillance video stills from KeyBank from July 26,
23 2015, showing WILEY driving a silver Infiniti SUV bearing California license plate
24 number 7ETY706. The video stills show the vehicle at a drive-up ATM, and shows
25 WILEY completing six transactions over a period of four minutes utilizing three cards
26 ending in 02451, 02469, and 63580. The cards ending in 02451 and 02469 were issued
27 in the name of “Shumika.” The card ending in 63580 was issued in the name of WILEY.

28 91. According to California DOL the registered owner of the silver Infiniti is
PV Holdings, which is the parent company of Avis rentals. PV Holdings provided rental

1 records showing this vehicle to be a Gray 2014 Infiniti QX70 rented by "Shumika" from
2 July 3, 2015, to August 3, 2015, for \$3,645.83, which was paid with a VISA card ending
3 in 5545. In addition, PV Holdings records indicate during the aforementioned rental
4 period, this vehicle was driven 3,301 miles. As discussed earlier, "Shumika" is the named
5 individual on KeyBank debit cards used by WILEY during attempted transactions at
6 various Fred Meyer, KeyBank ATMs, and Walmart.

7 92. On July 25, 2015 at approximately 11:47 p.m., a card ending in 02451 was
8 used to purchase two Western Union money orders for \$499. Surveillance photos
9 provided by a Fred Meyer investigator show WILEY conducting this transaction. This
10 card was loaded between approximately July 24, 2015, through July 26, 2015, with funds
11 via 24 fraudulent refund transactions totaling approximately \$4,799. These transactions
12 were processed using a merchant ID belonging to the Hometown Buffet restaurant
13 located in Temple City, California.

14 93. From 11:53 p.m. on July 25, 2015, to 12:00 a.m. on July 26, 2015, a card
15 ending in 02519 was used in four separate transactions. Two of the transactions were for
16 Western Union money orders totaling \$911.74. These transactions were declined. The
17 other two transactions, totaling \$8.74, were approved. Surveillance photos provided by a
18 Fred Meyer investigator show WILEY conducting these four transactions. This card was
19 issued on July 24, 2015, in the name of "Shumika." This card was loaded on July 25,
20 2015, with funds via 12 fraudulent credit transactions totaling approximately \$2,399.
21 These transactions were processed using a merchant ID belonging to the Hometown
22 Buffet outlet located in Temple City, California.

23 94. From 10:50 a.m. on July 25, 2015, to 10:51 a.m. on July 26, 2015, a card
24 ending in 02469 was used in two separate transactions. The two transactions were ATM
25 withdrawals from the Andover Park KeyBank branch. Each transaction was for \$500
26 totaling \$1,000. Surveillance photos provided by a KeyBank investigator show WILEY
27 conducting these transactions. This card was issued in the name of "Shumika." This card
28 was loaded between approximately July 24, 2015, through July 26, 2015, with funds via

1 24 fraudulent credit transactions totaling approximately \$4,799. These transactions were
2 processed using a merchant ID belonging to the Hometown Buffet restaurant located in
3 Temple City, California.

4 95. On July 26, 2015, a card ending in 10402 was used in two separate
5 transactions at a Renton, Washington, Fred Meyer store for Western Union money orders
6 totaling \$1,495. These transactions were declined. Surveillance photos provided by a
7 Fred Meyer investigator show WILEY conducting these transactions. This card was
8 issued in the name of WILEY. This card was loaded between approximately July 25,
9 2015, through July 27, 2015, with funds via 34 fraudulent refund transactions totaling
10 approximately \$6,799. These transactions were processed using merchant IDs belonging
11 to the Hometown Buffet outlet located in Temple City, California.

12 96. On July 26, 2015, at approximately 10:51 a.m., a card ending in 02451 was
13 used to make a \$500 withdrawal through the drive-thru ATM located at 275 Andover
14 Parkway West, Tukwila, Washington. Surveillance photos provided by a KeyBank
15 investigator show WILEY conducting this withdrawal. Additionally, WILEY is wearing
16 the same clothing he wore while making the Renton Fred Meyer transaction on July 26,
17 2015. This is the same card described in paragraph 92 above, which was loaded between
18 approximately July 24, 2015, through July 26, 2015, with funds via 24 fraudulent refund
19 transactions totaling approximately \$4,799. These transactions were processed using a
20 merchant ID belonging to the Hometown Buffet restaurant located in Temple City,
21 California.

22 97. On July 26, 2015, at approximately 1:31 p.m., a card ending in 63580 was
23 used to conduct a \$500 transaction at the Walmart #2571 located in Federal Way,
24 Washington. Surveillance photos provided by a Walmart investigator show WILEY
25 conducting this transaction. Additionally, WILEY is depicted on surveillance video
26 arriving and departing in the rented silver Infiniti. This card was issued in the name of
27 WILEY. This card was loaded on approximately July 24, 2015, through July 26, 2015
28 with funds via 24 fraudulent refund transactions totaling approximately \$4,799. These

1 transactions were processed using a merchant ID belonging to Hometown Buffet located
2 in Temple City, California.

3 98. On July 26, 2015, at approximately 1:41 p.m., a card ending in 02451 was
4 used to conduct a \$9.37 transaction at the Walmart #2571, the same Walmart described in
5 the previous paragraph. Surveillance photos provided by a Walmart investigator show
6 WILEY conducting this transaction. This card was issued in the name of "Shumika."
7 This is the same card described in paragraphs 92 and 96 above.

8 99. On July 26, 2015, at approximately 1:55 p.m., a card ending in 10428 was
9 used to conduct a \$960.70 transaction at the customer service desk at Walmart #2571, the
10 same Walmart described in the previous two paragraphs. Surveillance photos provided
11 by a Walmart investigator show WILEY conducting this transaction. This card was
12 issued in the name of WILEY. This card was loaded between approximately July 25,
13 2015, and July 27, 2015, with funds via 42 fraudulent refund transactions totaling
14 approximately \$8,399. These transactions were processed using a merchant ID belonging
15 to the Hometown Buffet restaurant located in Temple City, California.

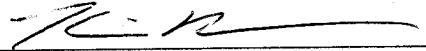
16 100. On July 25, 2015, at approximately 1:53 p.m., WILEY was recorded on
17 surveillance video at the Renton Fred Meyer attempting to purchase a Western Union
18 money order for \$500 using a credit card ending in 02519. This transaction was declined.
19 WILEY attempted a similar transaction minutes later using the same card. This card was
20 issued by KeyBank in the name of "Shumika." This is the same card described in
21 paragraph 93 above.

22 101. Investigators have identified at least 4,282 fraudulent transactions
23 conducted during the course of the scheme that can be tied directly to LILLARD,
24 WELLS, WILEY, SANDERS, "Shumika" or individuals known to be associated with
25 them during the course of this and/or previous schemes.


26 102. The scheme to date has exposed the various victims to a total potential loss
27 of at least \$2,222,495, with an estimated total loss to the various victims of at least
28 \$1,433,832. For example, between June 18, 2015, and July 1, 2015, the scheme

1 conducted approximately 1700 transactions leaving one victim—Green Dot Bank—
2 exposed to approximately \$748,743 in potential losses.

3 103. Based on the foregoing, I respectfully submit that probable cause exists to
4 believe that LILLARD, WELLS, WILEY, and SANDERS did conspire to knowingly
5 execute and attempt to execute a scheme or artifice to defraud a financial institution, and
6 to obtain money, funds, and other property owned by and under the custody and control
7 of a financial institution by means of false and fraudulent pretenses and representations,
8 all in violation of Title 18, United States Code, Sections 1344 and 1349.

9
10
11 
12 KEVIN BRENNAN
13 Special Agent
14 Federal Bureau of Investigation

15 SUBSCRIBED and SWORN to before me this 4th day of January, 2016.

16
17 
18 Brian A. Tsuchida
19 United States Magistrate Judge
20
21
22
23
24
25
26
27
28